Docket No. 00-022-MIS

CLAIMS:
What is claimed is:

Sub 91

1. A method for securing a transaction comprising:
receiving a request for a digest from a requestor;
retrieving a master key;
retrieving unique client information;
creating the digest by hashing the unique client information and the master key; and
returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with a third party.

2. The method recited in claim 1 above, wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information.

3. The method recited in claim 1 above, wherein the request includes unique merchant information which is used to access the master key.

4. The method recited in claim 1 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

5. The method recited in claim 1 above, wherein creating the digest by hashing is performed by a smart card.

09569757.060900

6. The method recited in claim 1 above further comprises encrypting the unique client information prior to retrieving the unique client information.

7. The method recited in claim 1 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

8. A method for securing a transaction comprising:

receiving, into a smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving unique client information, from the smart card memory;

retrieving a master key, the master key being known to a credit card issuer;

creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing the billing digest, the unique merchant information and the unique client information to the requestor.

0959897.0054500

9. The method recited in claim 8 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the credit card issuer.

10. The method recited in claim 8 above further comprises encrypting the unique client information and the unique merchant information prior to passing the information to the merchant.

11. A method for securing a transaction comprising:

sending a data transmission to a client's smart card, wherein the data transmission includes unique merchant information and a request for a billing digest;

receiving the billing digest, the unique merchant information and unique client information from the client's smart card, the billing digest being hashed from the unique merchant information, unique client information and secret information from the client's smart card; and

transmitting the unique merchant information and unique client information from the client's smart card to a credit card issuer.

12. The method recited in claim 11 above further comprises receiving a response from the credit card issuer.

13. A method for securing a transaction comprising:

receiving a transaction request from a requestor, wherein the request includes a digest and unique client information;

accessing a master key based on the unique client information;

creating an authorization digest by hashing the unique client information and the master key;

comparing the authorization digest with the digest from the requestor; and

returning a response to the requestor, the content of the response being based on an outcome of the comparison of the authorization digest with the digest from the requestor.

14. The method recited in claim 13 above, wherein the request includes unique requestor information and creating the authorization digest further comprises hashing the unique requestor information.

15. The method recited in claim 13 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

16. The method recited in claim 15 above further comprises:

accessing all previously used reference numbers associated with the unique client information;

comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information.

17. The method recited in claim 13 above, wherein creating the authentication digest by hashing is performed by a smart card.

18. The method recited in claim 13 above further comprises decrypting the unique client information prior accessing the master key.

19. The method recited in claim 13 above, wherein the transaction is a credit card transaction and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

20. A method for securing a transaction comprising:

generating a billing digest in a customer's smart card, the billing digest being hashed from merchant information, customer information and a master key;

creating an authentication digest by the credit card issuer, wherein the authentication digest is hashed from the merchant information, customer information and a master key associated with the customer information;

comparing the authorization digest with the billing digest; and

authorizing a transaction based on the comparison of the authorization digest with the billing digest.

21. A method for securing a transaction comprising:

indexing a master key to an account identifier for an account, wherein the account is between a customer and a financial institution;

providing the master key to the financial institution and a smart card controlled by the customer;

passing transaction data through a third party, wherein the transaction data includes at least the customer account identifier, third party information and a billing digest which is created from the customer account identifier, the third party information and the master key.

22. A smart card for conducting secure transactions comprising:

a input/output mechanism;

a processor; and

a memory containing:

financial account information;

a master key;

functional hashing algorithm;

an executable application, for executing on the processor, for invoking the functional hashing algorithm, wherein the functional hashing algorithm creates a digest from the financial account information and the master key and further wherein the executable application transmits, via the input/output mechanism, the digest and the financial account information to a requestor.

23. A system for conducting secure transactions comprising:

a client smart card for creating a billing digest from a resident client information, a resident master key and imported merchant information;

a merchant system for requesting the billing digest and for passing secure transaction information and the billing digest to a financial institution, wherein the transaction information comprises the client information, and the imported merchant information; and

a financial institution for receiving the transaction information and billing digest and for authorizing a transaction by:

accessing a master key based on the client information;

creating an authorization digest from the master key, the client information and the merchant information; and

comparing the authorization billing digest with the billing digest.

24. A system for securing a transaction comprising:

receiving means for receiving a request for a digest from a requestor;

retrieving means for retrieving a master key;

retrieving means for retrieving unique client information;

creating means for creating the digest by hashing the unique client information and the master key; and

returning means for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with a third party.

25. The system recited in claim 24 above, wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information.

26. The system recited in claim 24 above, wherein the request includes unique merchant information which is used to access the master key.

27. The system recited in claim 24 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

28. The system recited in claim 24 above, wherein the creating means for creating the digest by hashing is performed by a smart card.

29. The system recited in claim 24 above further comprises encrypting means for encrypting the unique client information prior to returning the unique client information.

30. The system recited in claim 24 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

31. The system recited in claim 24 above further comprises:

fingerprint reading and identification means for reading a fingerprint and authorizing a client based on an identity of a client's fingerprint.

32. A system for securing a transaction comprising:

receiving means for receiving a transaction request from a requestor, wherein the request includes a digest and unique client information;

accessing means for accessing a master key based on the unique client information;

creating means for creating an authorization digest by hashing the unique client information and the master key;

comparing means for comparing the authorization digest with the digest from the requestor; and

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the authorization digest with the digest from the requestor.

33. The system recited in claim 32 above, wherein the request includes unique requestor information and creating the authorization digest further comprises hashing the unique requestor information.

34. The system recited in claim 32 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

35. The system recited in claim 34 above further comprises:

accessing means for accessing all previously used reference numbers associated with the unique client information;

comparing means for comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information.

36. The system recited in claim 32 above, wherein creating the authentication digest by hashing is performed by a smart card.

37. The system recited in claim 32 above further comprises decrypting the unique client information prior accessing the master key.

38. The system recited in claim 32 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

39. A computer program product for securing a transaction embodied on a computer readable medium comprising:

receiving instructions for receiving a request for a digest from a requestor;

retrieving instructions for retrieving a master key;

retrieving instructions for retrieving unique client information;

creating instructions for creating the digest by hashing the unique client information and the master key; and

returning instructions for returning the digest and the unique client information to the requestor, wherein

the digest and the unique client information will be used for transacting with a third party.

40. A computer program product for securing a transaction embodied on a computer readable medium comprising:

receiving instructions for receiving, into a smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving instructions for retrieving unique client information, from the smart card memory;

retrieving instructions for retrieving a master key, the master key being known to a credit card issuer;

creating instructions for creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing instructions for passing the billing digest, the unique merchant information and the unique client information to the requestor.